#4

Patent
Attorney's Docket No. 030681-291

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	
A-jung KIM	Group Art Unit: 2131
Application No.: 09/816,080	Examiner: Unassigned
Filed: March 26, 2001	
For: KEY AGREEMENT METHOD IN SECURE COMMUNICATIONS SYSTEM USING MULTIPLE ACCESS METHOD	

CLAIM FOR CONVENTION PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

The benefit of the filing date of the following prior foreign application in the following foreign country is hereby requested, and the right of priority provided in 35 U.S.C. § 119 is hereby claimed:

Republic of Korea Patent Application No. 00-15035

Filed: March 24, 2000

In support of this claim, enclosed is a certified copy of said prior foreign application. Said prior foreign application was referred to in the oath or declaration. Acknowledgment of receipt of the certified copy is requested.

Respectfully submitted,

BURNS, DOANE, SWECKER & MATHIS, L.L.P.

Date: June 12, 2001

By: _____
Charles F. Wieland III
Registration No. 33,096

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620

KOREAN INDUSTRIAL PROPERTY OFFICE

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

Application Number: Patent Application No. 00-15035

Date of Application: 24 March 2000

Applicant(s): Samsung Electronics Co., Ltd. et al.

4 November 2000

COMMISSIONER

1020000015035 2000/11/

[Document Name] Patent Application

[Application Type] Patent

[Receiver] Commissioner

[Reference No.] 0006

[Filing Date] 2000.03.24

[IPC] G06F

[Title] Key distributing method in secure communication system using multiplexed access manner

[Applicant]

[Name] Samsung Electronics Co., Ltd.
[Applicant code] 1-1998-104271-3

[Attorney]

[Name] Young-pil Lee
[Attorney's code] 9-1998-000334-6
[General Power of Attorney Registration No.] 1999-009556-9

[Attorney]

[Name] Hyok-gun Cho
[Attorney's code] 9-1998-000544-0
[General Power of Attorney Registration No.] 2000-002820-3

[Attorney]

[Name] Hae-young Lee
[Attorney's code] 9-1999-000227-4
[General Power of Attorney Registration No.] 2000-002816-9

[Inventor]

[Name] KIM, A Jung
[I.D. No.] 660121-2037322
[Zip Code] 137-030
[Address] 101-804 Nokwon Apt., Chamwon-dong, Seocho-gu, Seoul
[Nationality] Republic of Korea

[Request for Examination] Requested

1020000015035 2000/11/

[Application Order] We respectively submit an application according to Art. 42 of the Patent Law and request and examination according to Art. 60 of the Patent Law.

Attorney Young-pil Lee
Attorney Hyok-gun Cho
Attorney Hae-young Lee

[Fee]

[Basic page]	20 Sheet(s)	29,000 won
[Additional page]	4 Sheet(s)	4,000 won
[Priority claiming fee]	0 Case(s)	0 won
[Examination fee]	3 Claim(s)	205,000 won
[Total]	238,000 won	

[Enclosures]

1. Abstract and Specification (and Drawings)_1 copy

대 한 민 국 특 허 청
KOREAN INDUSTRIAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Industrial Property Office.

출 원 번 호 : 특허출원 2000년 제 15035 호
Application Number

출 원 년 월 일 : 2000년 03월 24일
Date of Application

출 원 인 : 삼성전자 주식회사
Applicant(s)

CERTIFIED COPY OF PRIORITY DOCUMENT

2000 년 11 월 04 일

특 허 청
COMMISSIONER

【서류명】 특허출원서
【권리구분】 특허
【수신처】 특허청장
【참조번호】 0006
【제출일자】 2000.03.24
【국제특허분류】 G06F
【발명의 명칭】 다중 접근 방식을 이용한 보안 통신 시스템에서의 키 동의 방법
【발명의 영문명칭】 Key distributing method in secure communication system using multiplexed access manner
【출원인】
【명칭】 삼성전자 주식회사
【출원인코드】 1-1998-104271-3
【대리인】
【성명】 이영필
【대리인코드】 9-1998-000334-6
【포괄위임등록번호】 1999-009556-9
【대리인】
【성명】 조혁근
【대리인코드】 9-1998-000544-0
【포괄위임등록번호】 2000-002820-3
【대리인】
【성명】 이해영
【대리인코드】 9-1999-000227-4
【포괄위임등록번호】 2000-002816-9
【발명자】
【성명의 국문표기】 김아정
【성명의 영문표기】 KIM,A Jung
【주민등록번호】 660121-2037322
【우편번호】 137-030
【주소】 서울특별시 서초구 잠원동 녹원아파트 101동 804호
【국적】 KR
【심사청구】 청구

【취지】 특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인
이영필 (인) 대리인
조혁근 (인) 대리인
이해영 (인)

【수수료】

【기본출원료】	20	면	29,000 원
【가산출원료】	4	면	4,000 원
【우선권주장료】	0	건	0 원
【심사청구료】	3	항	205,000 원
【합계】	238,000 원		

【첨부서류】 1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 다중 접근 방식을 이용한 보안 통신 시스템에서의 키 동의 방법을 개시한다. 다중 접근 방식의 보안 통신 시스템에서의 키 동의 방법은, (a) 제1 사용자측에서 소스로부터의 신호를 비트 시퀀스로 인코딩하여 전송하는 단계, (b) 제1 사용자의 합법적 상대자인 제2 사용자측에서 디코딩되어 수신된 신호를 측정하여 기록하는 단계, (c) 다른 송신자측으로부터 발생하는 상호 변조 잡음의 영향을 받는 수신기를 사용하는 제2 사용자측에서 적어도 전송률, 전송오율 및 보안 정도를 고려하여 측정 문턱값을 정하는 단계, (d) 제2 사용자가 미리정해진 문턱값 이상의 측정치를 갖는 비트의 신호만을 키로 채택하는 단계, (e) 제2 사용자가 제1 사용자에게 키로 채택된 비트의 값 대신에 몇번째 비트인지 그 번호만을 알려주는 단계 및 (f) 제1 및 제2 사용자는 알려진 소정 번째의 비트의 값을 키로 채택하여 공유하고, 나머지 비트의 값을 버리는 단계를 포함한다.

【대표도】

도 5

【명세서】

【발명의 명칭】

다중 접근 방식을 이용한 보안 통신 시스템에서의 키 동의 방법{Key distributing method in secure communication system using multiplexed access manner}

【도면의 간단한 설명】

도 1은 본 발명이 적용되는 일반적인 통신 시스템의 통신 채널의 구조를 설명하기 위한 블럭도이다.

도 2는 실제 암호화 통신 시스템에서 비밀 키 공유시의 암호화 및 암호 해제 구조를 설명하기 위한 블럭도이다.

도 3은 광 CDMA 방식을 이용한 암호 통신 시스템에서 인코더/디코더의 구현 예를 설명하기 위한 도면이다.

도 4 (a) 및 (d)는 시간 지연된 CDMA 방식의 암호 통신 시스템에서 각 지점에서의 펄스 신호의 시간적 변화를 나타낸 도면이다.

도 5는 본 발명에 의한 보안 통신 시스템에서의 키 동의 방법을 설명하기 위한 플로우챠트이다.

도 6은 본 발명에 의한 키 동의 방법을 광 CDMA 방식에 적용하였을 경우에 채택된 키 스트링에서의 에러율을 나타낸 도면이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<7> 본 발명은 비밀 키 공유에 의한 암호화에 관한 것이며, 다중 접근 방식을 이용한 보안 통신 시스템에서의 키 동의 방법에 관한 것이다.

<8> 최근 들어 통신서비스가 폭발적으로 증가하고, 정보화 사회가 도래함에 따라 전송 대역폭과 보안성이 중요한 관건으로 대두되고 있다. 특히, 전자 상거래, 전자 금융 거래 및 네트워크 정보 서비스와 같이 전자 인증, 서명, 식별을 필요로 하는 시스템 구조가 증가함에 따라, 개인의 정보를 보호받고자 하는 요구가 증가하면서 암호화의 중요성이 더욱더 부각되고 있다.

<9> 암호 시스템에서 데이터는 합법적 사용자인가 비합적인 사용자인가를 불문하고 임의의 사용자가 입수 가능한 알고리즘에 의해 인코딩 및 디코딩된다. 따라서, 시스템의 보안성은 합법적 사용자에게만 이용가능한 키에 의해 좌우된다. 보안성이 보장된 암호화를 위해서 암호화 함수의 입력으로 사용되는 키의 설치, 보관 및 관리가 중요한 포인트라 할 수 있다.

<10> 종래의 암호화는 대부분 소프트웨어로 처리하는 범주에 머무르고 있어 외부의 물리적 공격이나 성능이 우수한 컴퓨터를 이용한 역암호화 키 추출 및 도청에 대한 방어력이 취약하다.

<11> 또한, 종래의 암호 통신에서 보안성있는 통신을 위해서는 평문(plain text)을 스크램블(scramble)하는 암호화 함수의 입력 변수로 키가 필요하다. 비밀 키의 전달이나 동

의를 사적인 채널을 이용하여 실행하는데 아무리 물리적으로 견고한 채널이라 할지라도 도청 등 외부의 공격에 대하여 파손되어 노출될 위험성이 존재한다. 이때, 도청자나 공격자는 태핑(tapping)한 비트에 대한 측정 결과로 키를 탐지해내거나 원래의 전달 키를 복원하여 다시 보내는 것도 가능하기 때문에, 공격이 발생하였을 시에도 합법적인 사용자들은 그 내용이 도청당하고 있다는 사실을 알 수 없다.

<12> 한편, 공개된 키를 사용하는 공용 키 시스템은 수학적 계산의 복잡성에 근거하고 있다. 최근 들어 계산의 병렬 수행, 새로운 알고리즘 구현 등이 가능하게 되면서 광 컴퓨터, 양자 컴퓨터에 대한 연구가 활발해지고 있으며, 이는 공용 키 시스템의 보안성에 큰 위협 요소로 대두되고 있다.

<13> 예를 들어, 알고리즘을 이용한 방식으로서, 공용 키 및 냅색(public key and knapsack) 방식 (US 4,218,582)이나 RSA(Rivest, Shamir and Adleman)5,829)이 있으며, 이들은 복잡한 수학계산을 필요로 한다. 또한, 수학적 계산의 복잡성에 근거하지 않는 암호 시스템으로 양자 암호학에 의한 키의 전달(US 5,307,410, US 5,515,438)을 들 수 있다. 그러나, 이러한 양자 암호학 시스템은 수행을 위해 매우 적은 파워의 코히어런트 상태(coherent state)에 있는 빛의 사용을 전제로 하기 때문에 실용적인 시스템에 사용되기에는 어려움이 많다.

【발명이 이루고자 하는 기술적 과제】

<14> 본 발명이 이루고자 하는 기술적 과제는, 전술한 문제점들을 해결하기 위해 창출된 것으로서, 다중 접근 방식을 사용하는 통신 시스템에서 사용자의 통신 시스템을 변형하지 않고 그대로 사용하면서, 보안성이 확립된 키의 동의를 물리적 계층에서 실현함으로써, 불법적 사용자의 도청 행위를 간단한 방법으로 무력화하며, 안

전한 키의 통신을 보장하여 보안성을 증대시키는, 다중 접근 방식의 보안 통신 시스템에서의 키 동의 방법을 제공하는데 있다.

【발명의 구성 및 작용】

<15> 상기 기술적 과제를 이루기 위하여, 다중 접근 방식을 이용한 보안 통신 시스템에서의 키 동의 방법은,

<16> (a) 제1 사용자측에서 소스로부터의 신호를 비트 시퀀스로 인코딩하여 전송하는 단계, (b) 제1 사용자의 합법적 상대자인 제2 사용자측에서 디코딩되어 수신된 신호를, 다른 송신자측으로부터 발생하는 상호 변조 잡음의 영향을 받는 수신기를 사용하여 측정하여 기록하는 단계, (c) 제2 사용자가 적어도 전송률, 전송오율 및 보안 정도를 고려하여 측정 문턱값을 정하는 단계, (d) 제2 사용자가 미리정해진 문턱값 이상의 측정치를 갖는 비트의 신호만을 키로 채택하는 단계, (e) 제2 사용자가 제1 사용자에게 키로 채택된 비트의 값 대신에 몇번째 비트인지 그 번호만을 알려주는 단계 및 (f) 제1 및 제2 사용자는 알려진 소정 번째의 비트의 값을 키로 채택하여 공유하고, 나머지 비트의 값을 버리는 단계를 포함한다.

<17> 이하, 본 발명에 의한 다중 접근 방식을 이용한 보안 통신 시스템에서의 키 동의 방법을 첨부한 도면을 참조하여 다음과 같이 설명한다.

<18> 먼저, 암호 통신 시스템에서 비밀 키를 공유하는 방법에 대해 간략히 설명한다.

<19> 일시적으로 보안성이 있는 통신을 하는 유선 통신기 또는 정보 보호 방식이 구현되지 않은 무선 단말기와의 통화를 위해서, 사용자가 통신 시작시에 미리 약속

된 특정 키가 입력하면, 송신측 단말기가 보안 모드로 설정 또는 해제되고, 특정 키를 수신한 단말기측도 송신측과 동일하게 보안 모드로 설정 또는 해제된다. 정상적인 통신, 더 나아가 도청등의 불법 행위로부터 안전한 통신이 가능하도록 한다. 이러한 특정 키를 이용한 보안 모드의 설정은 통신 셋업이 이루어지기 전에 알려주는 방법을 사용하거나, 통신 셋업이 이루어진 후에 통화중에 보안 모드의 설정 또는 해제가 이루어지도록 할 수 있다.

<20> 이때, 특정 키에 의한 보안 모드의 설정시에 사용하고자하는 블럭암호(blockcipher)의 비밀 키를 함께 전송하거나 비밀 키를 알아낼 수 있는 방법을 함께 전송할 수 있다. 송신측 암호화기와 수신측 암호 해제기에 사용되는 블럭암호는 물론 동일한 알고리즘과 동일한 비밀 키를 사용한다. 이를 위해서, 멀리 떨어져 있는 송신자와 수신자 사이에 비밀 키를 공유하는 방식이 필요하다.

<21> 비밀 공유 방식중 한 가지는 송신측에서 만들어낸 비밀 키를 보안 모드 설정시에 수신측에 전달하는 것이다. 즉, 보안 모드 설정시에 한 프레임의 비트를 보안 모드 설정을 의미하는 특정한 패턴으로 보낸 후에, 다음 프레임의 비트를 비밀 키로 하거나, 마스터 키로 암호화된 비밀 키로 하여 전송한다. 마스터 키를 사용할 경우에 모든 단말기는 동일한 마스터 키를 공유하며, 이 마스터 키는 신뢰있는 허가(trust authority)나 키 조건부 날인 증서(key escrow)등 책임있는 기관이 보관한다.

<22> 다른 방식은 송신측과 수신측 단말기내에 동일한 방식으로 저장되어 있는 키 집합들중 하나를 보안 모드 설정이 지정하는 것이다. 즉, 한 프레임의 정보 비트중 일부를 보안 모드 설정을 의미하는 특정 패턴으로 보내고, 나머지 비트를 비밀스럽게 저장된 비밀 키들의 인덱스로 사용하는 것이다. 이때, 저장된 비밀 키들은 무선 통신의 경우에

단말기 업체가 제공하는 비밀 키들과 가입자가 직접 입력한 비밀 키들로 구성된다.

<23> 이에 반해, 본 발명이 적용되는 방식은 별도의 채널을 통해 두 사용자가 비밀 키만을 교환한다. 이때, 교환되는 비밀 키는 사용자가 직접 입력하여 만들거나, 랜덤 넘버 발생 기능을 이용하여 만들어진 것을 이용한다. 이러한 방식으로 교환된 비밀 키는 전술한 두번째 방식을 이용하여 보안 모드 설정시에 지정되어 사용된다. 본 발명이 적용되는 방식은 특별히 물리적 보안 장치가 되어있지 않은 채널을 통해서도 두 사용자가 비밀 키를 교환, 공유할 수 있어 일반 통신기를 위한 암호 통신 시스템을 구축하는데 용이하다.

<24> 본 발명에 의한 암호 통신 시스템에서의 키 동의 방법은 종래의 통신 방식중 코드 분할 다중 접근(CDMA:Code Division Multiplexed Access)방식, 파장 분할 다중 접근(WDMA:Wavelength Division Multiplexed Access)방식 등 다중 접근 방식을 사용하는 근거리 통신망(LAN)이나 장거리 통신망(WAN)에서, 상호 채널간 발생하는 상호 변조 잡음이나 측정기의 잡음을 이용하여 불법적 사용자가 합법적 사용자와 서로 상관되지 않은 측정 결과를 얻게 함으로써 합법적 사용자간에 동의된 비밀 키를 정확히 예측하지 못하게 할 뿐만 아니라, 불법적 사용자가 비트를 훼손/재전송하면서 발생한 오염도를 측정함으로써 도청의 발생 여부와 그 정도를 가늠할 수 있게 한다.

<25> 도 1은 본 발명이 적용되는 일반적인 통신 시스템의 통신 채널의 구조를 설명하기 위한 블럭도로서, 통신 시스템은 키 발생자측의 인코더들(또는 변조기들)(102), 멀티플렉서(104), 전송 매체(110), 수신자측의 디코더들(또는 복조기들)(122), 디멀티플렉서(122), 검출기(124) 등을 포함한다.

<26> 도 1에 도시된 시스템을 비밀 키를 교환하는데 물리적 계층으로 이용한다. 합법적 사용자들중에서 키의 발생자인 제1 사용자는 해당 인코더(또는 변조기)(102)를 통해 신호 소스에서 발생한 신호를 다른 합법적 사용자들과 독립적으로 임의의 비트로 변조한 후에 전송한다. 이때, 합법적 사용자들 각각에 대해 전송될 각각의 신호는 멀티플렉서(또는 커플러)(104)를 통해 동일한 전송 매체를 공유하여 전송된다.

<27> 전송된 신호는 제2 사용자측에서 디멀티플렉서(또는 슬리터)(122)를 통해 분리되고, 해당 인코더(또는 복조기)(122)를 통과하며 필터링되어 채널이 선택되어진 후에 검출기(124)에서 측정된다. 여기서, 검출기(124)는 열 잡음, 쇼트 잡음, 전기 잡음등 내부적 잡음뿐만 아니라, 다른 채널의 신호에서 비롯된 상호 변조 잡음 등의 영향을 받는다.

<28> 이때, 인코더(또는 변조기)를 포함하는 변조 장치(미도시)는 인코더(또는 변조기)를 랜덤 비트 시퀀스 발생기(미도시)에 연결하여 전기적 신호 또는 광 신호를 랜덤한 비트의 데이타 시퀀스로 변조시키며, 복조 장치(미도시)는 위의 역 과정을 수행한다.

<29> 도 2는 실제 암호화 통신 시스템에서 비밀 키 공유시의 암호화 및 암호 해제 구조를 설명하기 위한 블럭도이다.

<30> 본 발명에 의한 키 동의 방법에 의해 합법적 사용자들간에 비밀 키(260)를 공유한 후에, 디지탈 암호 시스템(DES:Digital encryption System) 또는 삼중 DES와 같은 블럭 암호(270)를 이용하고, 암호화기(210)에서 암호 함수의 입력으로 비밀 키(260)를 적용하여 인코더(200)를 통과한 평문 내용을 암호화 한다. 다음에, 동기 디지탈 전송 방식(SDH:Synchronous Digital Hierarchy), CDMA등의 전송 방식에 따른 프레이머(framer)(220)를 이용하여 데이타 프레임을 만든다.

<31> 도 3은 광 CDMA 방식을 이용한 보안 시스템에서 인코더/디코더의 구현 예를 설명하기 위한 도면이다.

<32> N쌍의 사용자들간의 통신을 위해, N개의 인코더들이 병렬로 연결되어 있고, 그에 매치되는 N개의 디코더들이 병렬로 연결되어 있다. 제1 사용자의 신호 소스에서 발생한 신호는 CDMA 인코더, 프레이머를 통과하면서 랜덤한 비트의 시퀀스로 변조된다. 여기서, 신호 소스는 각 채널이 각각의 광원을 가지고 있거나, 여러 채널이 하나의 공유된 소스를 분리하거나 스펙트럼 슬라이싱하여 사용한다.

<33> 그 후에, 변조된 신호는 다른 사용자들에서 발생된 신호들과 함께 멀티플렉서에 입력되며, 공통의 전송 매체를 공유하여 전송된다. 전송된 신호들은 멀티플렉서를 통해 분리되어 각 수신단의 사용자에게 공급되고, 각각에 매치되는 디코더를 통해 필터링된 후에 검출된다.

<34> 각 인코더는 불균형 MZI(Mach-Zender Interferometer)와 같이 고유한 시간 지연을 초래하거나, 고유한 주파수만을 통과/반사시킬 수 있는 것처럼 고유한 코드에 맞게 진폭 또는 주파수를 할당하게 할 수 있는 장치이며, 여기서 각 인코더의 고유한 시간 지연은 소스의 간섭 시간보다 커야 한다.

<35> 각 디코더는 전술한 인코더에 매치되는 시간 지연 또는 코드 믹서를 가지고 있어, 신호를 타 신호와 구별할 수 있는 장치이다. 도 3 (a)는 시간 지연을 내부적(intrinsic)으로 발생시킬 경우를, 도 3 (b)는 시간 지연을 외부적(extrinsic)으로 발생시킬 경우를 각각 나타낸다.

<36> 도 4 (a) 및 (d)는 시간 지연된 CDMA 방식의 암호 통신 시스템에서 각 지점에서의

펄스 신호의 시간적 변화를 나타낸 도면이다.

<37> 도 4 (a)에 도시된 신호 소스로부터의 신호는 제1 사용자의 인코더로서의 경로차가 있는 간섭계의 두 암(arm)을 거치면서 도 4 (b)와 같이 시간 지연(τ 1)을 갖는 두개의 펄스로 분리된다. 그 후에, 제2 사용자의 디코더를 거치면서 4개의 펄스로 분리된다.

<38> 이때, 도 4 (c)와 같이 인코더와 디코더의 시간차가 일치할 경우에, 가운데 위치된 2개의 펄스가 서로 코히어런트하게 간섭을 일으켜 신호가 디코딩된다. 한편, 도 4 (d)와 같이 인코더와 디코더의 시간차가 일치하지 않을 경우에, 가운데 위치된 2개의 펄스는 펄스간에 시간적 상관성이 없으므로, 간섭을 일으키지 못하고 검출기에서 감지되지 못한다.

<39> 도 5는 본 발명에 의한 키 동의 방법을 설명하기 위한 플로우챠트이다.

<40> 본 발명의 기본 동작 원리는 첫째, 잡음에 민감한 약한 세기의 신호를 전송하여 외부 공격자로 하여금 전송된 신호 값을 구별하기 어렵게 하는 것이다. 둘째, 외부 공격자로 하여금 사용자와 서로 상관 관계가 없는 결과를 얻도록 하기 위해, 배경 잡음 또는 측정기 잡음 등과 같이 상관 관계가 없는 잡음을 이용한다.

<41> 구체적으로 도 5를 참조하면, 먼저 제1 사용자측에서 인코더를 통해 소스로부터의 신호를 임의의 비트 비퀀스로 변조하여 전송한다(제500단계). 제1 사용자의 인코더와 매치된 제2 사용자의 디코더를 통해 필터링되어 수신된 신호의 값을 측정하여 기록한다(제502단계). 이때, 제500단계에서 전송된 신호는 잡음에 민감한 약한 세기의 신호이며, 제502단계에서 기록된 측정치는 상호 변조 잡음, 배경 잡음 또는 측정기 잡음으로 인해 실제 전송된 신호를 중심으로 분산되어 분포된다.

<42> 다음에, 제2 사용자가 미리정해진 문턱값 이상의 측정치를 갖는, 값이 확실한 비트의 신호만을 키로 채택한다(제504단계). 다음에, 제2 사용자는 제1 사용자에게 키로 채택된 비트의 값 대신에 몇번째 비트인지 그 번호만을 알려준다(제506단계). 제1 및 제2 사용자는 알려진 소정 번째의 비트의 값을 비밀 키로 채택하여 공유하고, 나머지 비트의 값을 버린다(제508단계).

<43> 제508단계 후에, 사용자들간에 공유된 키 스트링중에서 임의의 부분 집합 비트들을 선택하여 패러티 체크 또는 에러 체크를 수행한다(제510단계). 에러율이 허용치안에 포함되는가를 판단한다(제512단계). 에러율이 허용치를 초과하였을 경우에, 전송에 보안성이 결여되어 도청의 가능성이 있다고 보고, 채택된 비트의 값을 폐기하고, 제500단계로 진행하여 새로운 전송을 수행한다.

<44> 한편, 에러율이 허용치안에 포함될 경우에, 그때의 전송을 보안성이 성립되었다고 본다. 허용 에러율이 얻어졌을 경우에, 에러 정정이나 해쉬 함수를 이용한 증폭을 수행하여 정제된 키 스트링을 얻는다(제514단계). 전술한 방법으로 공유한 키를 비밀 키로 하여 통신상의 내용을 암호, 암호 해제한다(제516단계).

<45> 제500단계에서 잡음에 민감한 약한 세기의 신호를 전송하면, 사용자의 측정치에도 많은 에러를 발생시킬 수 있다. 이를 보완하기 위해서, 제504~508단계에서 사용자가 미리정해진 문턱값 이상의 측정치를 갖는 비트의 신호만을 키로 채택하고, 나머지는 버림으로써 사용자의 측정치 에러를 줄일 수 있다.

<46> 한편, 제500단계에서 전송 매체를 통해 전송되는 동안에, 도청자 즉, 외부 공격자는 개입할 수 있다. 도청자가 전송된 데이타를 측정할 경우에, 이때에도 상호 변조 잡음 또는 도청자의 측정기 잡음으로 인해 측정치는 실제로 전송된 신호를 중심으로 분산

되어 분포된다. 그러나, 합법적 사용자들과 도청자는 서로 독립적인 측정기를 사용하고, 따라서 측정되는 결과에 영향을 미치는 잡음 또한 서로 상관 관계없이 독립적으로 작용한다. 따라서, 도청자의 측정기 잡음이 제2 사용자와 상관 관계없이 독립적으로 작용하기 때문에, 도청자측에서의 측정치는 제2 사용자측에서의 측정치에 상관없이 다른 값을 가질 수 있다.

<47> 더구나, 몇번째의 비트의 값이 키로 채택될지 모르기 때문에, 모든 측정치 즉, 문턱값 이하의 측정치를 갖는 비트의 결과도 이용하게 되고, 합법적 사용자들보다 훨씬 많은 에러를 보유한 키 스트링을 얻게 된다. 또한, 도청자는 문턱값을 초과하지 않는, 값이 확실하지 않은 비트를 포함하여 모든 비트에 대해 측정해야 하므로, 에러율이 높아지게 된다.

<48> 이와 같이 도청자가 개입에 성공하지 못하였을 경우에, 도청자는 제2 사용자와의 상관 관계를 높이기 위해서 제2 사용자에게 재전송할 수 있다. 도청자측에서의 높은 에러율의 전파로 인해 제2 사용자측에서의 측정치상에 기대치보다 높은 에러율이 발생한다. 따라서, 제510단계에서와 같이 에러 체크를 수행하였을 경우에, 도청의 여부를 가려낼 수 있다.

<49> 예컨대, 도 2에서 지배적인 잡음 요소는 원하지 않는 다른 송신기의 신호가 제2 사용자의 수신기에 비팅(beating)을 일으켜 발생하는 상호 변조 잡음이다. 매치되지 않는 송신기로부터의 상호 간섭을 고려하여 본 발명에 의한 키 동의 방법을 적용하였을 경우에, 도청자의 키 스트링에서의 에러율은 다음 수학식 1과 같이 나타낼 수 있다.

<50> 【수학식 1】

$$P_e^E \left(\frac{1}{2} erfc \left(\frac{1}{\sqrt{4N^2 E R I N E B_R}} \right) \right.$$

<51> 여기서, N은 다중 접근하는 사용자 쌍의 수이고, RIN은 상대적 세기 잡음(relative intensity noise)이고, B_R은 수신기의 대역폭이다. 수신측 사용자가 문턱값을 θ로 정하고, 그 이상의 측정치만을 키로 채택하였다고 가정한다. 이때, 상호 변조 잡음으로 인해 수신측 사용자의 키 스트링에 발생된 에러율은 도청자가 없는 정상 상태인 경우(P_e^B)와, 도청자가 개입하여 도청한 후에 재전송하였을 경우($\overline{P}_e^B$)에 다음 수학식 2와 같이 나타낼 수 있다.

<52> 【수학식 2】

$$P_e^B\left(\frac{1}{2}\,erfc\left(\frac{\theta/\sqrt{E}+1}{\sqrt{4N^2ERINEB_R}}\right)\right.$$

$$P_e^B\left(\frac{1}{4}\,erfc\left(\frac{1}{2N\sqrt{RINEB_R}}\right)erfc\left(\frac{\theta/\sqrt{E}-1}{2N\sqrt{RINEB_R}}\right)\right.$$

$$+\frac{1}{2}\left\{1-\frac{1}{2}\,erfc\left(\frac{1}{2N\sqrt{RINEB_R}}\right)\right\}erfc\left(\frac{\theta/\sqrt{E}+1}{2N\sqrt{RINEB_R}}\right)$$

<53> 여기서, E는 전송 신호의 진폭을 나타낸다.

<54> 예컨대, 4쌍의 수신자가 통신할 경우에, RIN = -100dB/Hz이고 , θ = 3E½로 설정하였다면, 사용자의 키 스트링의 에러율은 0.025인 반면 도청자의 키 스트링의 에러율은 0.26이 된다. 또한, 상관 관계를 높이기 위해, 도청자가 자신의 측정 결과를 토대로 재전송하면, 사용자의 키 스트링의 에러율은 0.17 정도로 증가하므로, 이 에러율의 변화치가 데이타의 오염도를 나타낼 수 있어 도청의 발생 여부를 짐작할 수 있게 한다.

<55> 문턱값을 높게 책정할 수록 보안성은 증진되지만, 많은 비트를 버려야 하기 때문에 그 대가로 전송 속도(data rate)가 감소하게 된다. 즉, 데이타 속도는 다음 수학식 3과 같이 나타낼 수 있다.

<56> 【수학식 3】

$$R\,(\,NE\frac{1}{2}\,erfc(\frac{\theta_N/\sqrt{E}-1}{2N\sqrt{RINEB_R}})$$

<57> 허용 에러율이 0.025라 할때, 2쌍의 사용자의 경우에 허용 에러율을 만족시키기 위한 문턱값은 θ=E½인데 반해, 4쌍의 사용자의 경우에 허용 에러율을 만족시키기 위한 문턱값은 3배 정도로 높게 책정되어야 한다. 그 결과, 데이타 속도는 0.62배 감소하게 된다. 따라서, 보안성과 많은 사용자의 수용을 위해서 높은 문턱값이 요구되고, 이는 전송 속도를 제한하는 요인이 될 수 있다.

<58> 도 6은 본 발명에 의한 키 동의 방법을 광 CDMA 방식에 적용하였을 경우에 채택된 키 스트링에서의 에러율을 나타낸 도면이다.

<59> 점선은 도청 오염이 있을 때의 수신측 사용자의 경우 θ=E½로 정했을 때를, 실선은 도청자의 경우 θ=3E½로 정했을 때를 각각 나타낸다. 사용자 수가 정해지면, 일정 허용 에러율을 만족시키기 위한 문턱값을 도출해낼 수 있다. 보안성을 위해서는 높은 문턱값이 요구되지만, 데이타 속도와 트레이드 오프를 고려하여 정할 수 있다.

【발명의 효과】

<60> 이상에서 설명한 바와 같이, 본 발명은 물리적 계층에서 보안성을 구축하므로 종래의 알고리즘을 이용한 방식과 달리 복잡한 수학 계산을 필요로 하지 않고, 이에 따라 후 신호 처리 역시 간단할 뿐만 아니라 알고리즘 형태 방식의 나약성이 배제되었고, 처리 전단계인 전송 단계에 적용할 경우에 비밀 키를 사용하여 블럭 단위의 신호에 보안 기능을 제공하는 방식에 블럭 암호의 보안성을 한층 더해 줄수 있다.

<61> 본 발명은 도청자나 제3의 불법적 사용자가 합법적 사용자와 동일한 키를 입수할

수 없을 뿐만 아니라, 시스템에서의 도청 발생 여부와 그 정도를 가늠할 수 있다. 도청자가 재발송시 수신한 데이터에서 발생한 에러를 탐지하고, 실험적 환경에서 기대되는 에러율과 비교함으로써, 데이터가 도청으로 어느 정도 오염되었는가를 감지할 수 있다. 합법적 사용자와 도청자간의 관측치에 서로 상호관계가 없도록 유도한다는 기본 원리는 광통신뿐만 아니라, 종래의 유무선 통신에 그대로 적용될 수 있으며, 그 응용 범위는 무궁 무진할 것이다.

<62> 또한, 본 발명은 시스템의 잡음을 이용함으로써, 어떠한 시스템상의 잡음도 이용가능하므로 적용가능한 통신 체제는 무궁무진하고, 고품도와 고수준의 장비 개발을 전제하지 않고, 설치가 용이하고 종래 설치이외에 부가 장치가 필요 없으며 즉시 적용가능하다. 따라서, 별도의 채널없이 일반 통신 시스템을 일시적으로 비밀 키 전달 채널로 활용한 후에, 보안 모드시 공유 키를 암호화하여 통신 보안을 할 수 있다.

<63> 특히, CDMA 방식을 이용한 경우에, 다수의 사용자가 타이밍 동기화(timing synchronization)할 필요없이 동시에 모든 주파수 대역을 공용한 채 비동기 전송을 하면서도 보안성과 안정성이 향상되어 일반 전송 시스템을 그대로 키 동의뿐 아니라, 암호문을 전송한 보안 시스템으로 재사용가능하고, 양방향 통신과 용이한 주소 교환이 가능한 실용적 시스템을 구축할 수 있다.

<64> 또한, 본 발명은 신호 증폭이 불가능한 양자 암호학에 반해 신호 증폭이 가능하므로, LAN 환경에서 다중 접근 방식의 적용뿐 만 아니라, WAN 환경에서도 다중 접근 방식의 적용도 가능하다.

【특허청구범위】

【청구항 1】

다중 접근 방식의 보안 통신 시스템에서의 키 동의 방법에 있어서,

(a) 제1 사용자측에서 소스로부터의 신호를 비트 시퀀스로 인코딩하여 전송하는 단계;

(b) 상기 제1 사용자의 합법적 상대자인 제2 사용자측에서 디코딩되어 수신된 신호를 측정하여 기록하는 단계;

(c) 제2 사용자가 미리정해진 문턱값 이상의 측정치를 갖는 비트의 신호만을 키로 채택하는 단계;

(d) 제2 사용자가 상기 제1 사용자에게 키로 채택된 비트의 값 대신에 몇번째 비트인지 그 번호만을 알려주는 단계; 및

(e) 제1 및 제2 사용자는 알려진 소정 번째의 비트의 값을 키로 채택하여 공유하고, 나머지 비트의 값을 버리는 단계를 포함하는 것을 특징으로 하는 키 동의 방법.

【청구항 2】

제1항에 있어서, 상기 (e) 단계 후에,

(f) 제1 및 제2 사용자들간에 공유된 키 스트링중에서 부분 집합 비트들을 선택하여 에러 체크를 수행하는 단계;

(g) 에러율이 허용치안에 포함될 경우에 에러 정정 과정을 거쳐 정제된 키 스트링을 얻고, 상기 단계들을 거쳐 공유한 키를 비밀 키로 동의하는 단계; 및

(h) 에러율이 허용치를 초과할 경우에 상기 (e) 단계에서 채택된 키를 폐기하고, 상기 (a)로 진행하는 단계를 더 포함하는 것을 특징으로 하는 키 동의 방법.

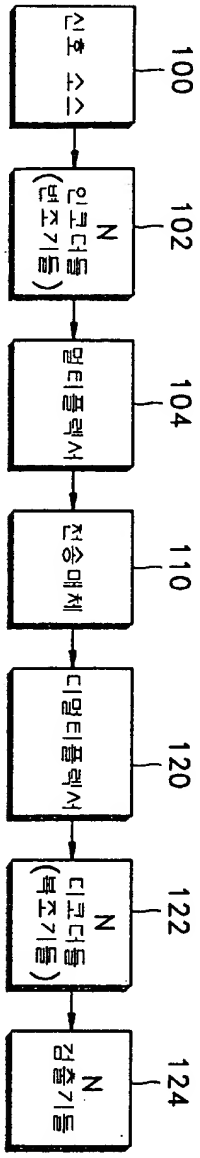
【청구항 3】

제1항에 있어서, 상기 (a) 단계에서 전송된 신호는 잡음에 민감한 신호이며,

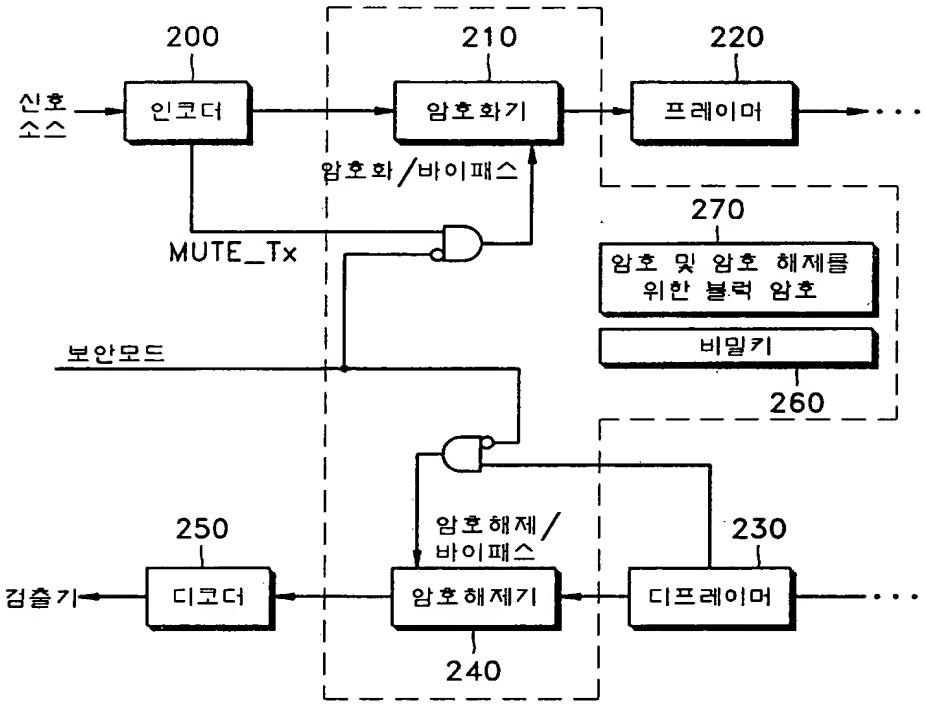
상기 (b) 단계에서 기록된 측정치는 제2 사용자측에서 신호 측정에 영향을 주는 적어도 측정기 잡음 및 상호 변조 잡음을 포함한 것을 특징으로 하는 것을 특징으로 하는 키 동의 방법.

【도면】

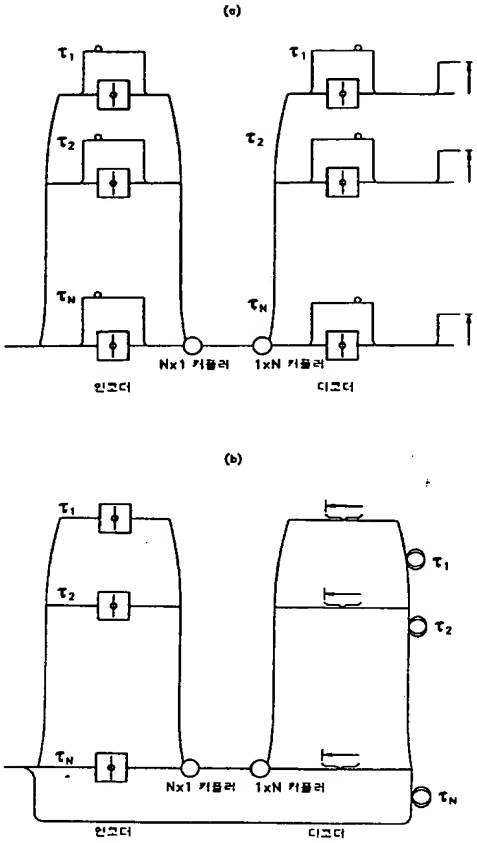
【도 1】


신호 소스
100
N 인코더들 (변조기들)
102
멀티플렉서
104
전송매체
110
디멀티플렉서
120
N 디코더들 (복조기들)
122
N 검출기들
124

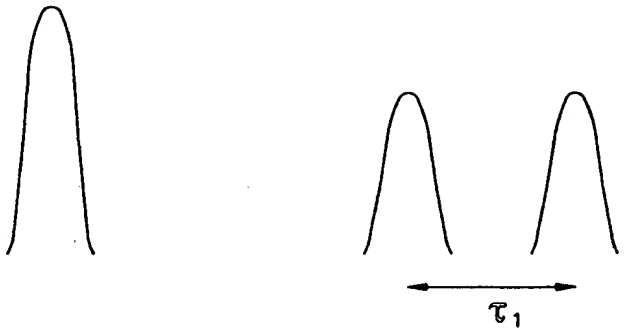
【도 2】


200
210
220
신호 소스
인코더
암호화기
프레이머
암호화/바이패스
MUTE_Tx
270
암호 및 암호 해제를 위한 블럭 암호
비밀키
260
보안모드
250
230
암호해제/바이패스
검출기
디코더
암호해제기
디프레이머
240

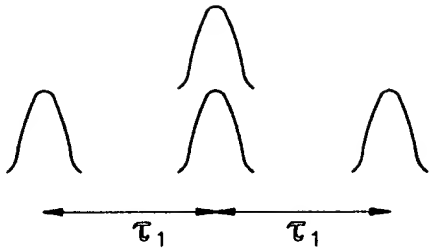
【도 3】


(a)
τ1
τ2
τN
Nx1 커플러
1xN 커플러
인코더
디코더
(b)
τ1
τ2
τN
Nx1 커플러
1xN 커플러
인코더
디코더

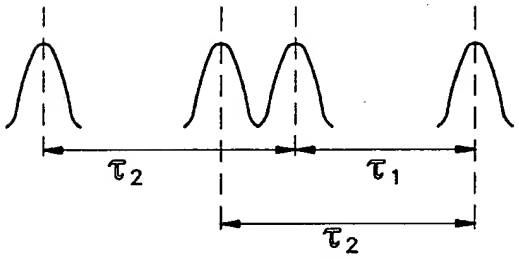
【도 4】



(a) 소스로부터의 신호 (b) 인코더의 결과

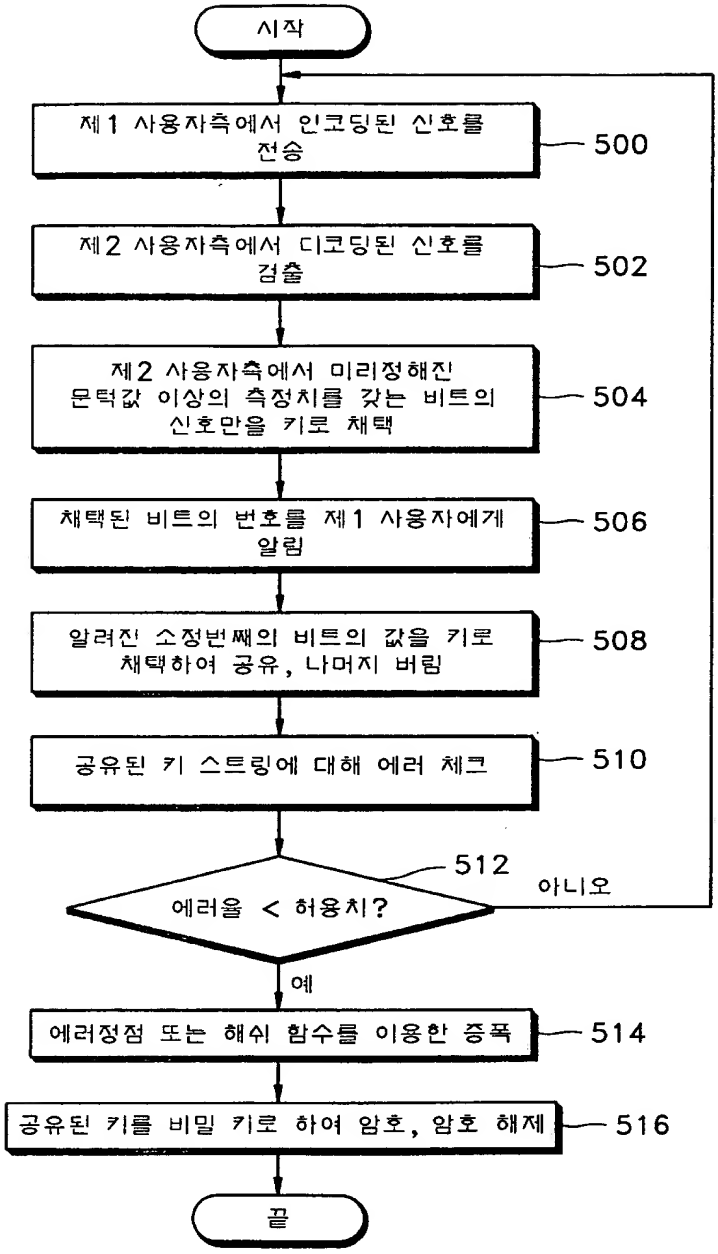


(c) 매치된 디코더의 결과

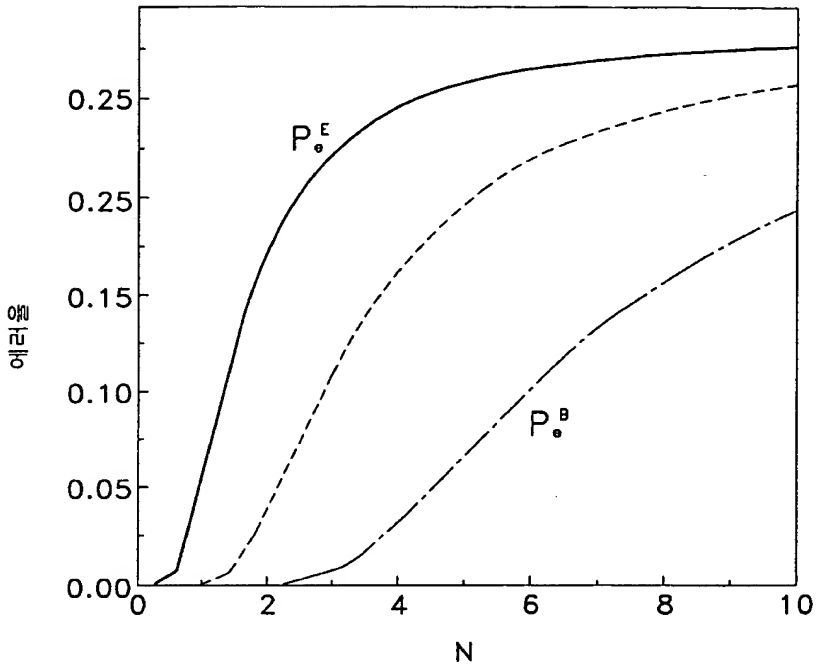


(d) 매치되어 않은 디코더의 결과

【도 5】


시작
제1 사용자측에서 인코딩된 신호를 전송
500
제2 사용자측에서 디코딩된 신호를 검출
502
제2 사용자측에서 미리정해진 문턱값 이상의 측정치를 갖는 비트의 신호만을 키로 채택
504
채택된 비트의 번호를 제1 사용자에게 알림
506
알려진 소정번째의 비트의 값을 키로 채택하여 공유, 나머지 버림
508
공유된 키 스트링에 대해 에러 체크
510
512
에러율 < 허용치?
아니오
예
에러정점 또는 해쉬 함수를 이용한 증폭
514
공유된 키를 비밀 키로 하여 암호, 암호 해제
516
끝

【도 6】



R=1GHz
RIN=−100dB/Hz